Auftragsverarbeitungsvertrag

Kunde

nachstehend **“Verantwortlicher”** genannt

und

MeisterLabs GmbH
Zugspitzstraße 2
85591 Vaterstetten
Germany

nachstehend “Auftragsverarbeiter” genannt

einzeln als **“Partei”**, gemeinsam als **“Parteien”** bezeichnet

schließen den folgenden Auftragsverarbeitungsvertrag (**“AVV”**) über die Datenverarbeitung zur Regelung der Verarbeitung personenbezogener Daten ab.

1 Präambel

1.1 Dieser AVV bildet einen Anhang zu den Allgemeinen Geschäftsbedingungen, die auch für diese Vereinbarung gelten, sofern in diesem AVV nicht anders angegeben wird.

1.2 Mit der Annahme der Allgemeinen Geschäftsbedingungen haben der Verantwortliche und der Auftragsverarbeiter diesen AVV als Teil der Click-through-Vereinbarung akzeptiert, um sicherzustellen, dass die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt.

2 Definitionen

2.1 "Datenschutzgesetze" umfassen die Allgemeine Datenschutzgrundverordnung der EU (EU/2016/679) ("**DSGVO**") sowie alle nationalen Datenschutzgesetze und -bestimmungen, die die Datenverarbeitungstätigkeiten im Rahmen dieses AVV regeln.

2.2 "Personenbezogene Kundendaten" umfassen alle personenbezogenen Daten, die der Auftragsverarbeiter und etwaige von ihm eingesetzte Sub-Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß dieses AVV verarbeiten.

2.3 Alle in diesem AVV verwendeten Begriffe sind im Sinne der EU-DSGVO, sofern nicht ausdrücklich etwas anderes vereinbart wurde.

3 Rechte und Pflichten des Verantwortlichen

3.1 Der Verantwortliche verpflichtet sich, die personenbezogenen Kundendaten, die dem Auftragsverarbeiter und entwaigen Sub-Auftragsverarbeitern übermittelt wurden, in Übereinstimmung mit den einschlägigen und anwendbaren Gesetzen und Vorschriften (insbesondere den Datenschutzgesetzen) zu verarbeiten.

4 Rechte und Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet

4.1 personenbezogene Kundendaten nur auf dokumentierte Anweisung des Verantwortlichen zu verarbeiten. Die Anweisungen für alle zur Vertragserfüllung notwendigen Verarbeitungsschritte gelten mit Vertragsabschluss als erteilt.

4.2 den Verantwortlichen unverzüglich zu benachrichtigen, wenn der Auftragsverarbeiter der Ansicht ist, dass die Anweisungen des Verantwortlichen gegen die geltenden Datenschutzgesetze verstoßen. Daraus ergibt sich jedoch keine Verpflichtung für den Auftragsverarbeiter, Rechtsberatung einzuholen. Ebenso wenig stellt die Erfüllung dieser Verpflichtung eine Rechtsberatung für den Verantwortlichen dar.

4.3 soweit dies möglich ist, den Verantwortlichen unverzüglich über alle Anfragen, Beschwerden, Meldungen, Anträge oder sonstigen Mitteilungen (im Folgenden als "**Antrag**" bezeichnet) zu informieren, die von einer Aufsichts- oder Regierungsbehörde oder einem sonstigen Dritten in

Bezug auf die Verarbeitung personenbezogener Kundendaten durch den Auftragsverarbeiter eingehen. Der Auftragsverarbeiter wird den Verantwortlichen in angemessener Weise unterstützen, damit dieser auf einen solchen Antrag in Übereinstimmung mit den geltenden Datenschutzgesetzen antworten kann. Die Beantwortung erfolgt ausschließlich durch den Verantwortlichen, es sei denn, der Auftragsverarbeiter ist nach zwingendem Recht verpflichtet, direkt zu antworten.

4.4 den Verantwortlichen angesichts der Art der Verarbeitung dabei zu unterstützen, seiner Verpflichtung zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO (EU/2016/679) genannten Rechte (zB Auskunft, Information, Berichtigung und Löschung, Datenübertragbarkeitl) in Bezug auf die Verarbeitung personenbezogener Kundendaten nachzukommen.

4.5 den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten (zB Datensicherheitsmaßnahmen, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffenen Personen, Datenschutz-Folgenabschätzung, Konsultation de Aufsichtsbehörde) in Bezug auf die Verarbeitung personenbezogener Kundendaten zu unterstützen, und zwar insbesondere

a) den Verantwortlichen so bald wie möglich schriftlich zu benachrichtigen, wenn der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit personenbezogenen Kundendaten erhält;

b) dem Verantwortlichen so bald wie möglich Informationen über die Verletzung des Schutzes personenbezogener Daten zu übermitteln.

4.6 alle personenbezogenen Kundendaten bei Beendigung dieses AVV oder des Hauptvertrags, unabhängig von den Gründen für die Beendigung, gemäß dieses AVV zu löschen. Wenn gesetzliche Verpflichtungen, an die der Auftragsverarbeiter gebunden ist, dies erfordern, kann der Auftragsverarbeiter im Einklang mit diesen Verpflichtungen eine Kopie der Daten des Verantwortlichen aufbewahren. Darüber hinaus ist der Auftragsverarbeiter berechtigt, alle erforderlichen Aufzeichnungen und Informationen (zu denen auch personenbezogenen Kundendaten gehören können), aufzubewahren, die er benötigt, um die Einhaltung seiner Verpflichtungen aus dem Hauptvertrag und dieses AVV unter Einhaltung der geltenden gesetzlichen Verjährungsfristen nachzuweisen.

4.7 Der Auftragsverarbeiter wird dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der in diesem AVV, dem Hauptvertrag oder den Datenschutzgesetzen festgelegten Pflichten nachzuweisen.

5 Sub-Auftragsverarbeiter

5.1 Der Verantwortliche erteilt hiermit seine allgemeine Zustimmung zur Beauftragung von Sub-Auftragsverarbeiter im Zusammenhang mit der Verarbeitung von Daten.

5.2 Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über jede Änderung hinsichtlich der Einschaltung oder Ersetzung weiterer Sub-Auftragsverarbeiter zu informieren. Sofern der Verantwortliche nicht innerhalb von zwei Wochen widerspricht, gilt die Einschaltung oder

Ersetzung als genehmigt. Im Falle eines Widerspruchs kann der Auftragsverarbeiter den AVV mit einer Frist von mindestens zwei Wochen kündigen. In diesem Fall ist der Auftragsverarbeiter nicht mehr verpflichtet, diejenigen Dienstleistungen zu erbringen, die die Verarbeitung personenbezogener Kundendaten im Auftrag des Verantwortlichen beinhalten. Die übrigen Bestimmungen des Hauptvertrags bleiben von der Beendigung des AVV unberührt.

5.3 Darüber hinaus ist der Auftragsverarbeiter verpflichtet

a) durch eine schriftliche Vereinbarung sicherzustellen, dass alle Sub-Auftragsverarbeiter im Wesentlichen an die gleichen Verpflichtungen gebunden sind, die für den Auftragsverarbeiter gemäß dieses AVV gelten.

b) die Haftung gegenüber dem Verantwortlichen zu übernehmen, wenn ein Sub-Auftragsverarbeiter seinen Datenschutzverpflichtungen aus der schriftlichen Vereinbarung im Sinne von Abschnitt a) nicht nachkommt.

6 Internationale Datenübertragungen

6.1 Der Auftragsverarbeiter kann personenbezogene Daten innerhalb des Europäischen Wirtschaftsraums ("**EWR**") oder in Ländern verarbeiten, die nach Auffassung der Europäischen Kommission ein angemessenes Schutzniveau gewährleisten.

6.2 Der Auftragsverarbeiter darf personenbezogene Daten an Sub-Auftragsverarbeiter, die in Ländern ansässig sind, die nach Ansicht der Europäischen Kommission kein angemessenes Datenschutzniveau gewährleisten, nur dann übermitteln, wenn der Auftragsverarbeiter sicherstellt, dass die in Kapitel V der DSGVO genannten Anforderungen eingehalten werden, insbesondere durch Abschluss von Modul 3 der von der EU-Kommission eingeführten Standardvertragsklauseln (Beschluss 2021/914/EU) mit dem Sub-Auftragsverarbeiter.

6.3 Sollten die von der EU-Kommission eingeführten Standardvertragsklauseln (Beschluss 2021/914/EU) für ungültig erklärt, ersetzt, für nichtig erklärt oder anderweitig so gestaltet werden, dass sie keine angemessenen Garantien für Datenübermittlungen in Drittländer mehr darstellen, verpflichten sich die Parteien, eine alternative Lösung zu finden, die mit den geltenden Datenschutzgesetzen im Einklang steht und die Rechtmäßigkeit der Übermittlung personenbezogener Daten in Drittländer gewährleistet.

7 Technische und Organisatorische Maßnahmen

7.1 Der Auftragsverarbeiter verpflichtet sich, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der geltenden Datenschutzgesetze in diesem AVV zu gewährleisten. Eine Übersicht über die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen ist in Anhang 2 enthalten. Der Verantwortliche bestätigt, dass die in Anhang 2 angeführten technischen und organisatorischen Maßnahmen angemessen sind.

7.2 Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle wesentlichen Änderungen der technischen oder organisatorischen Maßnahmen mitzuteilen. Der Auftragsverarbeiter stellt sicher, dass solche Änderungen nicht zu einem geringeren Schutzniveau führen.

8 Audit

8.1 Der Auftragsverarbeiter gestattet dem Verantwortlichen oder einem vom Verantwortlichen beauftragten unabhängigen Auditor, der auf Anweisung des Verantwortlichen handelt, Audits und Inspektionen in Bezug auf die Datensicherheit personenbezogener Kundendaten durchzuführen ("**Audit**"), um die Datenschutz- und Datensicherheitsverfahren im Rahmen dieses AVV zu überprüfen. Der Auftragsverarbeiter hat das Recht, einen Auditor abzulehnen, sofern er begründete Einwände gegen die Bestellung eines Auditors erhebt. Eine Ablehnung ist insbesondere dann gerechtfertigt, wenn der Auditor enge Verbindungen zu einem konkurrierenden Unternehmen hat oder wenn sonstige Gründe vorliegen, die Zweifel an der fachlichen Qualifikation oder der Unabhängigkeit des Auditors begründen.

8.2 Der Verantwortliche muss dem Auftragsverarbeiter ausnahmslos alle Audits, die sich auf die Verarbeitung personenbezogener Kundendaten beziehen, mit einer angemessenen Vorlaufzeit (in der Regel mindestens einundzwanzig Tage) schriftlich ankündigen und dabei die Uhrzeit, das Datum, die geplante Dauer und die Namen der Personen, die das Audit durchführen, angeben. Das Audit darf nur während der regulären Geschäftszeiten des Auftragsverarbeiters und ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters durchgeführt werden. Der Verantwortliche hat die Kosten für die Audits zu tragen.

8.3 Der Verantwortliche darf ein Audit höchstens einmal pro Kalenderjahr durchführen, es sei denn, es besteht ein begründeter Anlass für zusätzliche Audits.

9 Vertraulichkeit der Daten

Der Auftragsverarbeiter gewährleistet, dass die von ihm mit der Verarbeitung der persönlichen Kundendaten beauftragten Personen sich zur Vertraulichkeit verpflichtet haben oder gesetzlich zur Geheimhaltung verpflichtet sind.

10 Laufzeit und Kündigung

10.1 Dieser AVV tritt gemäß Punkt 1.2. in Kraft und gilt so lange, wie der Auftragsverarbeiter im Auftrag des Verantwortlichen personenbezogene Daten im Zusammenhang mit der Erbringung von Dienstleistungen im Rahmen des Hauptvertrags verarbeitet.

11 Allgemeine Bestimmungen

11.1 Zusatzabkommen bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformgebot.

11.2 Sollten der Verantwortliche und der Auftragsverarbeiter zusätzliche Vereinbarungen treffen, die im Widerspruch zu diesem AVV stehen, haben die Bestimmungen dieses AVV, die sich auf die Verarbeitung personenbezogener Kundendaten beziehen, vor allen entgegenstehenden Bestimmungen Vorrang.

Anhang 1

Wenn der Verantwortliche den Auftragsverarbeiter mit der Verarbeitung zusätzlicher personenbezogener Daten beauftragen möchte, die über die nachstehend genannten personenbezogenen Daten hinausgehen, muss er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird den Antrag prüfen und – wenn möglich – die Änderungen bestätigen.

Datensubjekte

Die verarbeiteten personenbezogenen Daten beziehen sich auf die folgenden Kategorien von Datensubjekten:

- Kunden des Verantwortlichen
- Kunden von Kunden des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Mitarbeiter von Kunden des Verantwortlichen
- Ansprechpartner von Lieferanten des Verantwortlichen
- Ansprechpartner von Lieferanten von Kunden des Verantwortlichen
- Interessenten des Verantwortlichen
- Interessenten von Kunden des Verantwortlichen

Datenkategorien

Die folgenden Datenkategorien werden verarbeitet:

- Personalstammdaten (zB Anrede, Nachname, Vorname, Anschrift, Titel, Beruf)
- Kommunikationsdaten (Telefonnummer, E-Mail-Adresse)
- Vertragsstammdaten (zB Vertragsbeziehungen, Produkt- und Vertragsinteressen)
- Kundenhistorie
- Vertragsstamm-,Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Technische Protokolldaten (zB Login, IP-Adresse, Zeitstempel)
- Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln: Freitextfeld-Eingaben im Rahmen der Erstellung von Mindmaps durch Benutzer, Freitextfeld-Eingaben im Rahmen der Planung von Tasks durch Benutzer, Dateien und Bilder, die im Rahmen der Erstellung von MindMaps und Tasks durch den Benutzer hochgeladen werden

Besondere Datenkategorien

Nein.

Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten und Datensubjekte

Der Auftragsverarbeiter bietet ein Online-Mindmapping-Tool an, mit dem Ideen visualisiert, entwickelt und geteilt werden können. Der Mindmap-Editor wird für das Brainstorming, die Strukturierung von Informationen, die Erstellung von Notizen und die Planung von Projekten beim Kunden verwendet.

Der Auftragsverarbeiter bietet ein Task-Management-Tool an, mit dem der Verantwortliche Projekte erstellen und Aufgaben an verschiedene Teammitglieder vergeben kann. Der Verantwortliche kann zudem Checklisten und Fristen in den Aufgaben verwalten, den Projektfortschritt einsehen und verfolgen.

Der Auftragsverarbeiter bietet ein Online-Dokumentation-Tool an, mit dem vom Verantwortlichen Notizen und Dokumente erstellt und mit Teammitgliedern geteilt werden können. Die Dokumente werden für Notizen, Checklisten, Präsentationen und die Weitergabe von Informationen an Mitarbeiter verwendet.

Umfang, Art und Zweck der Datenverarbeitung (beauftragte Leistungen):

- In Übereinstimmung mit der Definition in Art. 4 Nr. 2 der DSGVO

Der Auftragnehmer übernimmt das Hosting, die Wartung und den Support für die o. a. Online-Tools. Hierbei ist eine Zugriffsmöglichkeit auf personenbezogene Daten der Betroffenen nicht ausgeschlossen, soweit solche von den Nutzern in die Online-Tools eingegeben werden. Überdies stellt der Auftraggeber dem Auftragnehmer personenbezogene Daten zur Einrichtung der Nutzerkonten zur Verfügung.

Anhang 2 - Überblick über technische und organisatorische Maßnahmen

Datenschutz / Sicherheitskonzept

Die Datenschutzrichtlinien des Verantwortlichen und des Auftragsverarbeiters (einschließlich aller einschlägigen Sicherheitsrichtlinien) betreffen die Sicherheit personenbezogener Daten.

Organisatorische Sicherheitsmaßnahmen

Die interne Organisation ist so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

- Es gelten Richtlinien und Verfahren, welche regelmäßig geprüft werden.
- Risiken werden bewertet und dokumentiert.
- Informationen werden gemäß einer Richtlinie klassifiziert.
- Es wurde ein Security Manager ernannt.
- Geeignete Messungen der Leistung und Wirksamkeit des Sicherheitsmanagement werden durchgeführt.

Sicherheitsmaßnahmen bei Änderung eines Dienstes

Der Änderungsmanagement-Prozess umfasst eine Analyse der Auswirkungen auf den Datenschutz und eine Bewertung der Informationssicherheitsrisiken.

Personenbezogene Daten dürfen für die Prozess- oder Systementwicklung und die damit verbundenen Tests nur dann verwendet werden, wenn sie vor ihrer Verwendung anonymisiert oder anderweitig geschützt wurden.

Sicherheitsmaßnahmen in der Benutzerverwaltung

Maßnahmen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Passwörter werden mit einem Passwort Manager verwaltet.
- Es gibt eine Passwortrichtlinie, die durch den Passwort Manager und ein System zur Verwaltung mobiler Geräte verstärkt wird.
- Die Zwei-Faktor-Authentifizierung wird dort durchgeführt, wo es unsere Richtlinie verlangt.

Sicherheitsmaßnahmen für den logischen Zugriff

Der logische Zugriff auf personenbezogene Daten ist eingeschränkt.
Maßnahmen stellen sicher, dass die zur Nutzung der Datenverarbeitungssysteme berechtigten Personen nur auf die Daten zugreifen können, für die sie berechtigt sind.

- Der Zugriff wird nach dem Need-to-know-Prinzip (Erforderlichkeitsprinzip) gewährt.

- Der Zugriff wird auf Antrag gewährt/widerrufen. Der Widerruf kann auch automatisch nach einer bestimmten Zeitspanne oder manuell nach einer Überprüfung erfolgen.
- We Wir verfügen über ein Verfahren zur Beantragung von Genehmigungen, in dem der Benutzer, der Zugang benötigt, das System, die geforderten Genehmigungen, der Antragsteller und der Bevollmächtigte dokumentiert sind.
- Im Rahmen des HR-Onboarding- und des HR-Offboarding-Prozesses werden auch Zugriffsrechte gewährt/entzogen.
- Wir führen regelmäßige Überprüfungen des logischen Zugriffs auf alle unsere Systeme durch, abhängig von der Klassifizierung der Informationen, und dokumentieren diese Überprüfungen.

Aufteilung der Mandate

Die Kundendaten sind logisch aufgeteilt und durch Sicherheitsmechanismen voneinander getrennt. Darüber hinaus gibt es Test- und Staging-Systeme, die vollständig vom Produktivsystem getrennt sind.

Löschung von Daten

Die Daten werden aus der Datenbank oder dem Speicher gelöscht; die Backups werden nach 95 Tagen gelöscht.

Sicherheitsmaßnahmen für den physischen Zugang

Der physische Zugang zu personenbezogenen Daten in jedem Format ist begrenzt.

Personenbezogene Daten in jeglichem Format sind gegen versehentliche Offenlegung aufgrund von Naturkatastrophen und Umweltgefahren geschützt.

Personenbezogene Daten auf tragbaren Medien oder Geräten sind vor unbefugtem Zugriff geschützt. Sicherheitsmaßnahmen für Speichermedien verhindern unbefugtes Lesen, Kopieren, Ändern oder Entfernen von Speichermedien.

Google-Rechenzentrum (Frankfurt, Deutschland)

- Verschlüsselungsmaßnahmen und Zertifikate des Rechenzentrums:
  https://cloud.google.com/docs/security/encryption/default-encryption
  https://cloud.google.com/security/compliance/iso-27001/

MeisterLabs GmbH Büro (München, Deutschland)

- MeisterLabs GmbH Büro in München, Zugspitzstraße 2, 85591 Vaterstetten.
- Der Zugang zum Bürogebäude ist durch eine Außentür mit Schloss gesichert.
- Der Zugang zu den Büroräumen der MeisterLabs GmbH ist zusätzlich mit einem Schloss gesichert und nur mit den entsprechenden Schlüsseln möglich, die nur Mitarbeitern der MeisterLabs GmbH zur Verfügung stehen. Der Vermieter verfügt über keinen Schlüssel zu diesen Räumlichkeiten. Die Schlüssel werden den Mitarbeitern der MeisterLabs GmbH bei Vertragsabschluss ausgehändigt, bei Beendigung des Arbeitsverhältnisses wird der Schlüssel eingezogen. Zudem gibt es eine entsprechende Dokumentation über die im Umlauf befindlichen Schlüssel.
- Gäste oder Besucher werden in den beiden Büros der MeisterLabs GmbH nicht empfangen.
- Das Firmennetzwerk in den oben genannten Räumlichkeiten der MeisterLabs GmbH in München ist durch eine moderne Firewall geschützt.

Sicherheitsmaßnahmen für die Speicherung von Daten

Es gibt Maßnahmen, die eine unbefugte Eingabe sowie eine unbefugte Auswertung, Veränderung oder Löschung von gespeicherten personenbezogenen Daten verhindern. Dazu gehört auch der Schutz vor Schadsoftware.

- Cloud-Speicher
  - Die Daten werden auf Block-Ebene verschlüsselt, siehe “Sicherheitsmaßnahmen für den physischen Zugang”.
  - Der Zugang zu personenbezogenen Daten wird sorgfältig verwaltet, siehe “Sicherheitsmaßnahmen für den logischen Zugang”.
  - Die Computerressourcen in der Cloud werden automatisch auf Schwachstellen überprüft.
  - Ein Host Intrusion Detection System (HIDS) ist vorhanden, um ungewöhnliches Verhalten auf den Rechnern zu erkennen.
  - Tägliche Backups werden 14 Tage lang aufbewahrt, danach werden sie gelöscht.
- Mitarbeitergeräte
  - Alle Mitarbeitergeräte sind vollständig verschlüsselt. Eine Firewall und ein Virenschutz sind vorhanden. Automatische Bildschirmsperren sind aktiviert. Asset-Management-Prozesse sind implementiert. Alle Geräte sind in einer Mobile Device Management-Lösung registriert, um Richtlinien automatisch durchzusetzen.
  - Gestohlene oder verlorene Geräte können aus der Ferne gesperrt oder gelöscht werden.
  - Nur zugelassene Reparaturgeschäfte dürfen firmeneigene Geräte reparieren. Computer werden nur bei autorisierten Händlern gekauft.
  - Von der Speicherung von Daten auf Wechseldatenträgern wird abgeraten. Es gibt Richtlinien für die Entsorgung.

Sichere Entwicklungen

Es gilt die Secure Development Policy, um sicherzustellen, dass kein unsicherer Code eingeführt wird. Bestehende Codes und Bibliotheken von Drittanbietern werden regelmäßig auf Schwachstellen überprüft.

- Es gibt Maßnahmen zur Erkennung von unsicherem Code (statische Codeanalyse).
- Bei der Entwicklung muss unsere Secure Development Policy beachtet werden.
- Der gesamte Anwendungscode wird einer Peer Review unterzogen.
- Verwendete Bibliotheken werden automatisch auf bekannte Schwachstellen gescannt.

Sicherheitsmaßnahmen für die Dateneingabe

Es wird sichergestellt, dass überprüft werden kann, welche personenbezogenen Daten von wem und wann in die Datenverarbeitungssysteme eingegeben wurden.

Kontrolle der verarbeiteten Informationen

Das Datensubjekt hat die Möglichkeit, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten, sowie diese Daten berichtigen und löschen zu lassen.

Die Daten werden online direkt in der Datenbank oder im Onlinespeicher gelöscht und verschwinden nach 2 Wochen aus den Backups, sobald diese erneuert wurden.

Sicherheitsmaßnahmen bei der Verarbeitung

Es wird sichergestellt, dass die Daten im Falle einer Auftragsverarbeitung personenbezogener Daten nach den Anweisungen des Verantwortlichen verarbeitet werden.

Sicherheitsmaßnahmen bei der Übertragung von Daten

Es gelten Maßnahmen, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von personenbezogenen Daten während der Übertragung oder des Transports von Speichermedien verhindern.

- Alle Verbindungen zu unseren Rechenzentren werden während der Übertragung mit modernem TLS verschlüsselt. Die unter stützten Verschlüsselungen werden regelmäßig auf ihre Wertminderung überprüft.
- Dritte Parteien, die personenbezogene Daten verarbeiten, haben angemessene Sicherheitskontrollen eingerichtet.
- Unverschlüsselte E-Mail-Anhänge enthalten keine vertraulichen oder sensiblen Informationen.

Verfügbarkeit und Ausfallsicherheit

- Zertifikate des Rechenzentrums: https://cloud.google.com/security/compliance/iso-27001/
- Cloudflare als Diensteanbieter für DDoS-Schutz

Sicherheitsmaßnahmen für den Fall von Zwischenfällen

- Es wurde ein dokumentiertes Verfahren für den Umgang mit Datenschutzvorfällen und -verletzungen eingeführt.
- Die Mitarbeiter werden regelmäßig darin geschult, wie sie Sicherheitsvorfälle verhindern können, aber auch, wie sie auf solche Vorfälle reagieren können, einschließlich der möglichen Notwendigkeit, Vorfälle den Behörden zu melden und die Benutzer zu informieren.
- Es wurde eine interne Hotline für Sicherheits- und Datenschutzvorfälle eingerichtet. Die Mitarbeiter werden ermutigt, Vorfälle zu melden.

Bewertungen der Sicherheitsmaßnahmen

Bewertungen und Tests der Wirksamkeit der wichtigsten organisatorischen, technischen und physischen Schutzmaßnahmen zum Schutz personenbezogener Daten werden gemäß unserer Richtlinien durchgeführt, die unter anderem Folgendes beinhalten:

- Externe Schwachstellen-Scans und Penetrationstests werden mindestens einmal im Jahr durchgeführt.
- Externe Infrastrukturprüfungen werden mindestens einmal im Jahr durchgeführt.
- Externe Code-Prüfungen werden durchgeführt, wenn dies notwendig erscheint.
- Interne Architektur- und Sicherheitsprüfungen werden mindestens einmal im Jahr durchgeführt.

Die Ergebnisse der Analysen werden dokumentiert.

Anhang 3 - Zugelassene Sub-Auftragsverarbeiter

Mit Abschluss dieses AVV stimmt der Verantwortliche einer Beauftragung der nachstehend angeführten Sub-Auftragsverarbeiter zu:

Sub-Auftragsverarbeiter		Beschreibung der Verarbeitung (*einschließlich einer klaren Unterscheidung der Zuständigkeiten, falls mehrere Sub-Auftragsverarbeiter zugelassen wurden*)	
Name	**Anschrift**		**Verarbeitungsregion**
Bereitstellung von Meister-Produkten			
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Gewährleistung der **Produktbereitstellung** durch Produkt-Hosting in der Cloud-Region Europa. Bereitstellung von KI-Funktionen.	Frankfurt a.M., Deutschland
MeisterLabs Software GmbH	Mariahilferstraße 97, 1060 Wien, Österreich	Gewährleistung der **Produktfunktionalität**, insbesondere durch Produktwartung und -entwicklung	Wien, Österreich
SmartBear Software Inc.	450 Artisan Way, Somerville, MA 02145	Gewährleistung der **Produktfunktionalität** u.a. durch Fehlerbehebung mit Hilfe von Protokollen zur Behebung von Fehlern in Ausnahmefällen	USA
Cloudflare Inc.	101 Townsend Street, San Francisco, California 94107, U.S.A.	Gewährleistung der **Produktsicherheit**, insbesondere durch Schutz vor DDoS-Angriffen und Bereitstellung eines Content Delivery Network	EU (mehrere Regionen)

Unterstützung im Rahmen der Lizenz-Modelle Business und Enterprise			
MeisterLabs Inc.	89 Yesler Way, WA 98104 U.S.A.	Gewährleistung des Benutzer-Supports	USA
AirCall SAS	11-15 Rue Saint-Georges, 75009 Paris, France	Voice Over IP in Verbindung mit Support-Anfragen per Telefon	Frankfurt, Deutschland
Mailgun Technologies, Inc.	535 Mission St., 14th Floor, San Francisco, California 94105, USA	E-Mail-Dienstleister im Zusammenhang mit Support-Anfragen in schriftlicher Form	USA
Zendesk, Inc.	1019 Market Street, San Francisco, CA 94103, USA	Ticketing-System für die Organisation und Verwaltung von Supportanfragen	EU (Deutschland, Belgien)
Bereitstellung der KI-Funktionalität innerhalb der Meister-Produkte. Sie können die Nutzung der Meister KI-Funktionalität jederzeit in Ihren Kontoeinstellungen deaktivieren.			
OpenAI, LLC	3180 18th St., San Francisco, CA 94110, USA	Bereitstellung von KI-Funktionen in unseren Produkten	USA